(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 April 2001 (05.04.2001)

PCT

(10) International Publication Number
WO 01/24476 A1

(51) International Patent Classification[7]: H04L 29/06

(21) International Application Number: PCT/IB00/01304

(22) International Filing Date:
12 September 2000 (12.09.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/156,669 29 September 1999 (29.09.1999) US
09/551,811 18 April 2000 (18.04.2000) US

(71) Applicant: NORTEL NETWORKS LIMITED [CA/CA]; World Trade Center of Montreal, 380 St. Antoine Street West, 8th floor, Montreal, Quebec H2Y 3Y4 (CA).

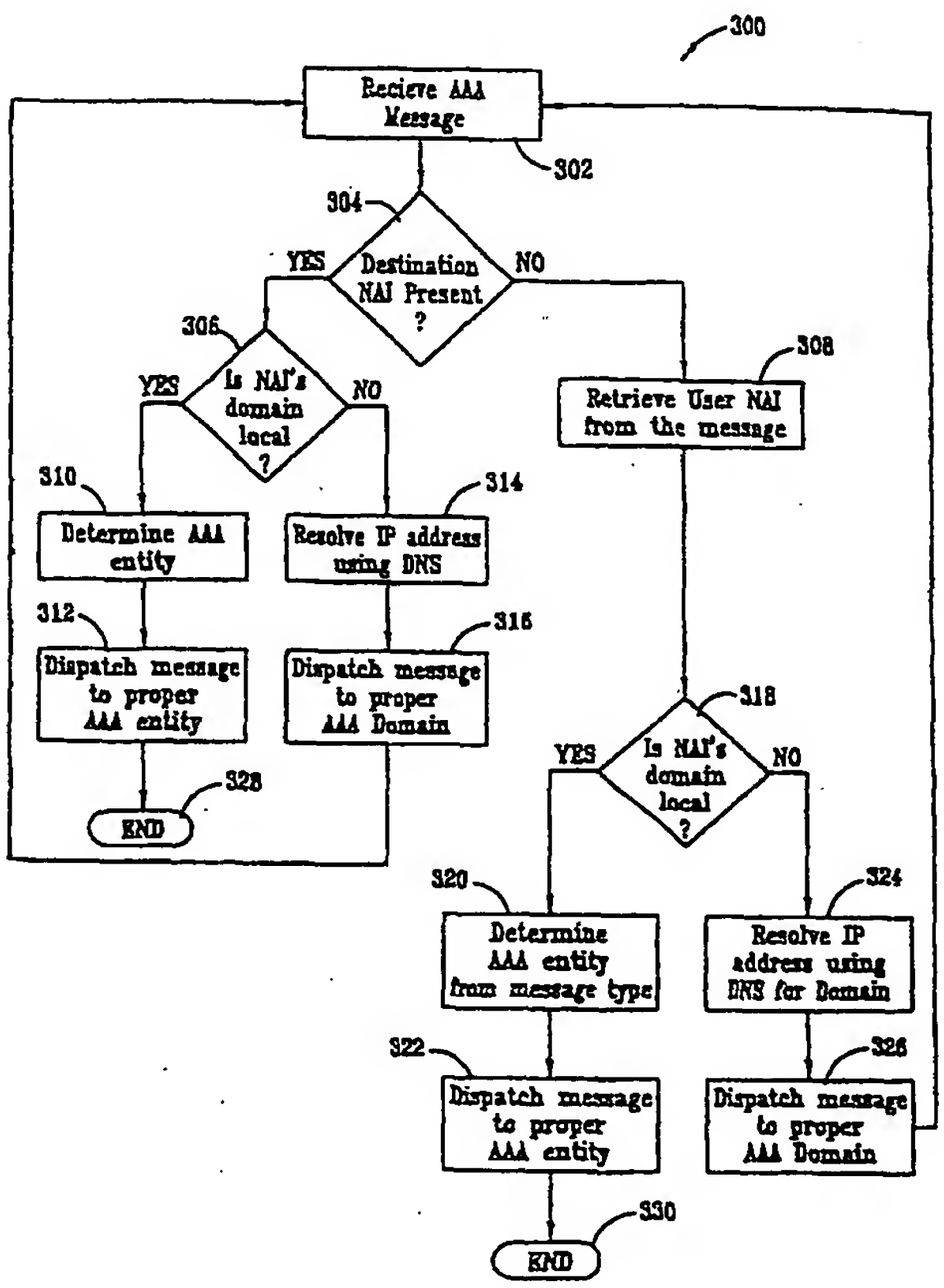
(72) Inventors: TUMMALA, Rambabu; 4324 Giovanni Dr., Plano, TX 75024 (US). QADDOURA, Emad; 1320 Wateredge Drive, Plano, TX 75093 (US). PATIL, Basavaraj; 409 Pedmore Drive, Coppell, TX 75019 (US). AKHTAR, Haseeb; 3102 Pamela Place, Garland, TX 75044 (US).

(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: APPARATUS AND METHOD FOR ROUTING AAA MESSAGES BETWEEN DOMAINS OF A NETWORK



(57) Abstract: AAA messages are routed among AAA entities in a data network coupled to a plurality of domains, each domain including at least one AAA server for routing AAA messages, and at least one AAA entity for serving users within each of the respective domains. AAA messages include a Source Network Access Identifier ("NAI") and optionally include a Destination NAI. An AAA message is received and a determination is made whether the message includes a Destination NAI. If no Destination NAI is present, a User NAI is retrieved from the message, and a determination is made whether the User NAI's domain is local, and routing the message accordingly. If the Destination NAI is present in the message, a determination is made whether the Destination NAI's domain is local, and the message is routed accordingly.

WO 01/24476 A1

Published:
— *With international search report.*
— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

APPARATUS AND METHOD FOR ROUTING AAA MESSAGES BETWEEN DOMAINS OF A NETWORK

TECHNICAL FIELD OF THE INVENTION

This invention relates generally to routing messages between domains of a network and, more particularly, to routing messages between domains of a network using Authentication, Authorization, and Accounting ("AAA") protocols.

BACKGROUND

Internet Protocol (IP) networks, such as the Internet, are generally apportioned into "domains," and each user of a network is typically assigned to one "home" domain within the network. Unfortunately, when a user is assigned to one home domain, it is often difficult and cumbersome for that user to then access the network through a "non-home" domain. This is because, when a user attempts to access the network through a non-home domain, the non-home domain is not configured to readily authenticate who the user is, and to determine what the user's home domain is, and what account the user is authorized to use with the home domain.

The difficulty users experience accessing the network through non-home domains is becoming more acute as users are becoming more mobile, traveling between domains, and desiring access to networks from any number of different locations, often not within the range of their home domain. Therefore, there is a growing need for technology, namely protocols, which will permit users to readily access a network from "non-home" domains. To this end, various protocols, referred to as Authentication, Authorization and Accounting ("AAA") protocols have been developed by Internet Service Providers (ISP's) which permit domains to

authenticate users of other domains, to identify the home domain and accounts held by users at their home domains, and to obtain authorization from the user's home domain for the user to use the identified account, as the user travels between domains of the Internet.

There are, however, a number of drawbacks associated with using conventional AAA protocols, many of which drawbacks are related to their failure to provide an adequate mechanism to route AAA messages among various AAA entities. Some of the drawbacks of conventional AAA protocols are that: 1) they provide routing based only on user network access identifiers ("NAIs"); 2) they support messaging only between a user's home domain and serving domain; 3) they do not allow communication between two or more non-home serving domains, such as during handoffs; 4) they do not allow specifically directed communication between two AAA entities; 5) they require that AAA entities have publicly routable, as opposed to private, IP addresses; and 6) they create potential security problems by virtue of modification of AAA messages by AAA servers by addition of a proxy state. With respect to item 5), conventional AAA protocols do not permit communication with a AAA entity behind a firewall or proxy server wherein the entity does not have a publicly routable IP address, but has only a private IP address.

Two embodiments of AAA protocols proposed by the Internet Engineering Task Force are referred to as RADIUS and DIAMETER. DIAMETER, for example, specifies that DIAMETER servers be stateless, meaning that DIAMETER servers should act strictly as routers for DIAMETER clients' messages without storing state information, such as the source or destination of the messages. Servers that do not store such state information are referred to as being "lightweight." According to recent drafts of the DIAMETER

protocol, AAA messages are routed according to a User NAI, which may be provided in a format such as "user@domainX.com". A User NAI is, in common terminology, a user's e-mail address. DIAMETER currently uses the domain of the user NAI (*e.g.*, domainX) to route messages, the domain also being referred to as the realm portion of the user NAI.

Conventional AAA servers, such as those employing DIAMETER and RADIUS, include the following fields in AAA messages for routing messages to their proper destinations:

1. User NAI;
2. Proxy State(only used when messages go through proxy servers); and
3. Command Code (*i.e.*, message type).

The User NAI identifies the user that the message is carried on behalf of. The Proxy State is a field used when a proxy server is used to forward AAA messages. The Command Code identifies the type of message.

FIGURE 1 depicts a communication network 100 commonly used in the prior art in connection with transmission and receipt of AAA messages. The network 100 includes a data network (such as the Internet) 102 that is coupled to a Domain A, a Domain B, and a Domain C. Domain A includes an AAA Entity 1 of Domain A, an AAA Entity 2 of Domain A, and an AAA Server of Domain A, which are operably interconnected to one another and also to the data network 102. In addition, Domain B includes an AAA Entity 1 of Domain B, an AAA Entity 2 of Domain B, and an AAA Server of Domain B, each of which is operably interconnected to one another and also to the data network 102. Similarly, Domain C includes an AAA Entity 1 of Domain C, an AAA Entity 2 of Domain C, and an AAA Server of Domain C, each of which is operably interconnected to one another and also to the data network 102.

The AAA servers of Domain A, Domain B, and Domain C are each responsible for delivering or routing AAA messages to appropriate entities, which perform task(s) specified by the messages. It is the responsibility of the AAA servers of Domain A, Domain B, and Domain C to resolve the appropriate server or entity to which to send the AAA messages. The AAA Entities 1 and 2 of Domain A, Domain B, and Domain C each serve users in their respective domains and are also used to forward messages between users and the AAA Entities' respective AAA servers.

The AAA Servers and AAA Entities illustrated in FIGURE 1 may comprise any conventional computer generally capable of receiving, storing, processing, and outputting data. While not shown in detail, the AAA Servers and AAA Entities each include components, such as input and output devices, volatile and non-volatile memory, and the like, but, because such computer components are well known in the art, they are not shown or described in further detail herein.

The drawbacks associated with conventional AAA protocols outlined above are discussed in more detail hereinbelow. For example, as an illustration of the first drawback mentioned above, suppose an AAA registration request of a user with a User NAI of name@DomainB.com is sent from the AAA Entity 1 of Domain A to the AAA Server of Domain A. In accordance with conventional protocols, the AAA Server of Domain A reads the realm portion of the User NAI of the message, determines that the message should be forwarded to the Domain B, and forwards the message to the AAA Server of Domain B. Upon receiving the message, the AAA Server of Domain B determines that the message is intended for an entity in its domain and then forwards the message to the appropriate AAA Entity, such as, for example, the AAA Entity 1 of Domain B. The AAA Entity 1 of Domain B then processes the message.

After the AAA Entity 1 of Domain B has processed the message, it will attempt to send a registration response message back to the AAA Entity 1 of Domain A. In so attempting, the AAA Entity 1 of Domain B forwards the registration response message to its AAA server, which is the AAA Server of Domain B. The AAA Server of Domain B will then attempt to forward the message to its proper destination, AAA Entity 1 of Domain A. However, the AAA server of Domain B cannot use the user NAI (i.e., name@domainB.com) to route the message to the AAA Entity 1 of Domain A, because to do so would direct the message to the AAA Entity 1 of Domain B as a result of the AAA Server of Domain B determining where to route the message based on the *domainB* realm of the User NAI. The User NAI does not include any information to tell the AAA server of Domain B that the user (i.e., name@domainB.com) has sought to register at a non-home domain (i.e., Domain A).

Under conventional AAA protocols, Domain B would use a Proxy State to send a message back to Domain A. Under such protocols, the AAA server of Domain B does not have the necessary information to forward the registration response message to the Domain A or, more particularly, to the AAA Entity 1 of Domain A. To properly route the registration response message, the AAA server of Domain B would need to maintain state information regarding the source of the original registration request message (i.e., AAA Entity 1 of Domain A) or use a Proxy State. However, the AAA server of Domain B cannot maintain this state information without running afoul of DIAMETER's requirement that all AAA servers be stateless.

The second and third drawbacks of conventional AAA protocols mentioned above can be exemplified by a user having a user NAI of user@domainB.com who connects via a wireless mobile link to the data network 102 through the

Domain A, for example, using a notebook computer or personal digital assistant. As the user moves from the Domain A to the Domain C, the Domain A and the Domain C will need to communicate with one another in order to facilitate a handoff of the user. However, conventional AAA protocols do not permit such communication because a message sent on behalf of the user to the Domain C in an effort to initiate the handoff would result in a response to the message based on User NAI by the Domain C being sent to the Domain B, because Domain B is the user's home domain, as indicated by the realm portion of the user's user NAI (i.e., "domainB"). Thus, communication between the two non-home serving domains (e.g., Domain A and Domain C) is not possible using conventional protocols.

The second and third drawbacks are also exemplified when a user with user NAI of user@domainC.com connected to the data network 102 via a wireless link travels from the Domain B to the Domain A and thus needs to be handed off to the Domain A. Conventional protocols do not permit a particular AAA entity newly assigned to serve the user (e.g., AAA Entity 2 of Domain A) to communicate with an AAA entity of Domain B that had been serving the user prior to the handoff request (e.g., AAA Entity 2 of Domain B). Rather, a message from the AAA Entity 2 of Domain A would be sent to the Domain C, because the Domain C is indicated as the user's home domain by virtue of the realm portion of the user's User NAI (i.e., "domainC").

The fourth and fifth drawbacks of conventional AAA protocols mentioned above are exemplified when the AAA Entity 2 of Domain A needs to communicate specifically with the AAA Entity 1 of Domain B, for example, because a roaming wireless Internet user moving between Domain A and Domain B needs to be handed off from the Domain A to the Domain B. Conventional AAA protocols do not permit such communication.

While conventional protocols *do* permit an entity in a non-home serving domain to specifically communicate with another entity in the user's *home* domain, they do not permit specific entities in two different non-home serving domains to communicate with one another. This problem is exacerbated when one or both of the entities is behind a proxy server or firewall, since conventional protocols require publicly-routable IP addresses. As is well known, an entity behind a proxy server or firewall does not have a publicly routable IP address, but, rather, only has a private IP address. This drawback of conventional protocols is due in part to their use of user NAIs for AAA message routing. In addition, if a host IP address has only a private address, the same drawback of conventional AAA protocols is present.

The sixth drawback is illustrated by the use of a proxy state by AAA servers to modify or mark AAA messages so that they can be routed. Under conventional protocols, a computer participating in the routing of a message is required to mark or modify the message in order to keep track of from where it received the message. For example, if computer 1 routes a message to computer 2, computer 2 will mark or modify the message to indicate that it came from computer 1. When computer 2 sends the message to computer 3, computer 3 will, on receipt of the message, mark or modify it as having been received from computer 2. This process of marking or modifying the message will continue until the message reaches its destination.

Such marking or modification of messages creates a security risk because it prevents the use of certain security mechanisms, such as IPSEC, which attempt to maintain message security by verifying whether a message has been modified. Thus, if routing computers modify or mark the message using a proxy state, the security mechanisms are

unable to verify that that the message has not been modified.

Thus, there is a need for an apparatus and method for routing AAA messages among various AAA entities in systems based on domains in which routing of AAA messages of roaming users is achievable, messaging between a AAA entity to another AAA entity in any domain can be performed, and communication between two or more non-home serving domains can be accomplished. There is a further need for an apparatus and method that permits communications between two specific entities in different domains as well as communications between entities in which one or more of the entities is behind a firewall or a proxy server and thus does not have a publicly-routable IP address. There is a further need for an apparatus and method that overcome the potential security problems associated with the use of a proxy state message modification to route AAA messages as in the prior art. There is also a need for AAA servers capable of meeting the above-described needs to be stateless and lightweight, since the RADIUS and DIAMETER protocols mandate that message state information not be stored in the servers.

SUMMARY OF THE INVENTION

In response to these and other limitations, provided herein are a unique method and apparatus for routing Authentication, Authorization, and Accounting ("AAA") messages in a communication system. The communication system comprises a data network coupled to a plurality of domains, wherein each domain includes at least one AAA server and at least one AAA Entity.

In one embodiment, routing an AAA message includes receiving the AAA message having a User NAI, determining whether the AAA message includes a Destination NAI, in

response to a determination that the AAA message includes a Destination NAI determining whether an NAI domain of the Destination NAI is or is not local. In response to a determination that the Destination NAI is local, the AAA message is dispatched to a local AAA entity identified by the Destination NAI. In response to a determination that the Destination NAI is not local, the AAA message is dispatched to an AAA server in a non-local domain identified by the Destination NAI. In other embodiments, in response to a determination that the NAI domain of the User NAI is non-local, the AAA message is dispatched to a non-local AAA entity identified by the User NAI.

In still other embodiments, an apparatus for routing AAA messages between AAA entities is provided. The apparatus comprises a first domain operably connected to the Internet that has at least one AAA server that is adapted to route a plurality of AAA messages having at least a Source NAI and a User NAI. The apparatus also includes a first AAA entity operably connected to the first domain that is adapted to send and receive a plurality of AAA messages having at least a Source NAI and a User NAI.

In other embodiments, a second domain operably connected to the Internet and having at least one AAA server that is adapted to route a plurality of AAA messages having at least a Source NAI and a User NAI is provided. The apparatus further includes an AAA entity operably connected to the second domain that is adapted to send and receive a plurality of AAA messages having at least a Source NAI and a User NAI.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention and the advantages thereof, reference is now made

to the following description taken in conjunction with the accompanying drawings, in which like reference numbers indicate like features and wherein:

FIGURE 1 is a diagram illustrating a prior art communications system used in connection with current AAA protocols and in connection with the present invention;

FIGURE 2 is a diagram illustrating an exemplary Registration Request message according to the present invention; and

FIGURE 3 is a flow diagram illustrating an algorithm for routing of AAA messages according to the present invention.

DETAILED DESCRIPTION

In the following discussion, numerous specific details are set forth to provide a thorough understanding of the present invention. However, it will be obvious to those skilled in the art that the present invention can be practiced without such specific details. In other instances, well-known elements have been illustrated in block diagram or schematic form in order not to obscure the present invention in unnecessary detail. Additionally, for the most part, details concerning routing of AAA messages and the like have been omitted inasmuch as such details are not necessary to obtain a complete understanding of the present invention and are within the skills of persons of ordinary skill in the relevant art.

Referring to FIGURE 1 of the drawings, the reference numeral 100 generally designates a communication network embodying features of the prior art. The network 100 includes a data network (such as the Internet) 102 that is coupled to a Domain A, a Domain B, and a Domain C. Domain A includes an AAA Entity 1 of Domain A, an AAA Entity 2 of

Domain A, and an AAA Server of Domain A, which are operably interconnected to one another and also to the data network 102. In addition, Domain B includes an AAA Entity 1 of Domain B, an AAA Entity 2 of Domain B, and an AAA Server of Domain B, each of which is operably interconnected to one another and also to the data network 102. Similarly, Domain C includes an AAA Entity 1 of Domain C, an AAA Entity 2 of Domain C, and an AAA Server of Domain C, each of which is operably interconnected to one another and also to the data network 102.

The AAA servers of Domain A, Domain B, and Domain C are each responsible for delivering or routing AAA messages to appropriate entities, which perform task(s) specified by the messages. It is the responsibility of the AAA servers of Domain A, Domain B, and Domain C to resolve the appropriate server or entity to which to send the AAA messages. The AAA Entities 1 and 2 of Domain A, Domain B, and Domain C each serve users in their respective domains and are also used to forward messages between users and the AAA Entities' respective AAA servers.

The AAA Servers and AAA Entities illustrated in FIGURE 1 may comprise any conventional computer generally capable of receiving, storing, processing, and outputting data. While not shown in detail, the AAA Servers and AAA Entities each include components, such as input and output devices, volatile and non-volatile memory, and the like; however, because such computer components are well known in the art, they will not be shown or described in further detail herein.

In FIGURE 2, an exemplary AAA Registration message 200 of the present invention is shown which facilitates the routing of AAA messages based on domains, using such AAA protocols as DIAMETER and RADIUS, and can be deployed in any type of network setup as either a Registration Request

message or as a Registration Response message (discussed below). The AAA Registration message 200 comprises a plurality of Attribute Value Pairs ("AVPs"), including: (1) a Source Network Access Identifier (NAI) field 202, (2) an optional Destination NAI field 204, (3) User NAI field 206, and (4) a Command Code field 208. The Source NAI field 202 is a required field used to identify the source from which a Registration message originates. The Destination NAI field 204 is an optional field used to identify the destination NAI a Registration message. The Registration message 200, when used to Request Registration, generally does not require the Destination NAI, but when used to Respond to a Registration Request, generally does require a Destination NAI, since the Destination NAI of a Registration Response message is most often the Source NAI of a Registration Request message. The User NAI field 206 field identifies the user and the user's home domain, and the Command Code field 208 identifies the type of message, for example, as a Registration Request, or as a Response to a Registration Request.

For example, in a preferred embodiment, if a mobile user who is roaming outside his home domain submits a Registration Message 200 to the AAA Server of a non-home domain to Request Registration at the non-home server, the Registration Message would include the Source NAI field 202, the User NAI field 206, and the Command Code field 208. The Source NAI field 202 identifies the source of the message as being an AAA entity of the non-home domain at which the user is requesting Registration. The User NAI field 206 identifies the user that originated the request, including the home domain of the user, even though the user is now requesting to be registered at the non-home domain. The Command Code field 208 identifies the type of message as a Registration Request.

Referring now to both FIGURES 1 and 2, if an AAA Entity 1 of Domain A submits a Registration Request message 200 to the AAA Server of Domain A on behalf of a user with a User NAI of user1@domainB, in a preferred embodiment, the message would include the following:

a. Source NAI field 202 (aaaentity1@DomainA);
b. Destination NAI field 204 (--empty--)
c. User NAI field 206 (user1@Domain B); and
d. Command Code field 208 (Registration Request).

The Destination NAI field 202 is empty, and the Source NAI field 202 identifies the source of the message 200 as being the AAA Entity 1 of Domain A, since the user is requesting Registration with the Domain A through the AAA Entity 1 of Domain A. The User NAI field 206 identifies the user that originated the request, which in this example is user1, who has a home domain of Domain B, but who is now requesting to be registered at Domain A. The Command Code field 208 identifies the type of message as a Registration Request.

FIGURE 3 is a flow diagram, designated by the reference numeral 300, depicting control logic implemented by an AAA server for routing AAA messages 200 in accordance with a preferred embodiment of the present invention. The control logic will be exemplified first with respect to the routing of a message 200, wherein a user (designated herein as "user1") having a home domain in Domain B is requesting Registration in Domain A.

Accordingly, in step 302, the AAA Server of Domain A receives a message 200 from the AAA Entity 1 of Domain A. Execution then proceeds to step 304, wherein the AAA Server of Domain A determines whether the message includes a Destination NAI in the field 204 of the Registration Message 200. If the AAA Server of Domain A determines that a Destination NAI is not present in the Destination NAI field

204, execution proceeds to step 308; otherwise, execution proceeds to step 306, discussed below with respect to a response to a request for registration. In step 308, the AAA Server of Domain A retrieves the User NAI field 206 from the message. Execution then proceeds to step 318, wherein a determination is made whether the User NAI's domain is local (*i.e.*, whether the user1 has the Domain B as its home domain). If it is determined that the User NAI's domain is not local, execution proceeds to step 324; otherwise, execution proceeds to step 320, discussed below. In step 324, the Internet Protocol ("IP") address of the NAI domain is resolved using the well-known Domain Name System ("DNS"). Execution then proceeds to step 326. In step 326, the message is dispatched to the proper domain (*e.g.*, Domain B). Execution then returns to step 302.

In step 302, the AAA Server of Domain B receives the message sent to Domain B from the AAA Server of Domain A in step 326 above. Execution then proceeds to step 304, wherein the AAA Server of Domain B determines whether a Destination NAI is present in the field 204. If it is determined that a Destination NAI is not present in the field 204, execution proceeds to step 308; otherwise, execution proceeds to step 306, discussed below with respect to a response to a request for registration. In step 308, the AAA Server of Domain B retrieves the User NAI 206 from the message 200. Execution then proceeds to step 318, wherein the AAA Server of Domain B determines whether the domain of the User NAI 206 is local (*i.e.*, whether the user1 has the Domain B as its home domain). If it is determined that the User NAI's domain is local, execution proceeds to step 320; otherwise, execution proceeds to step 324,

discussed above. In step 320, the AAA Server of Domain B determines from the Command Code field 208 that the message 200 is a Request for Registration. Execution then proceeds to step 322, wherein the message 200 requesting registration is sent to the appropriate entity of Domain B, which is, for example, the AAA Entity 1 of Domain B. Execution then terminates at step 330.

Referring now to FIGURES 1 and 2, if the AAA Entity 1 of Domain B submits to the AAA Entity 1 of Domain A a message 200 responding to a request for registration, the message 200 would, in a preferred embodiment, include the following fields:

a. Source NAI field 202 (aaaentity1@DomainB)

b. Destination NAI field 204 (aaaentity1@DomainA)

c. User NAI field 206 (user1@DomainB)

d. Command Code field 208 (Registration Response)

The Source NAI field 202 identifies the source of the message as the AAA Entity 1 of Domain B. The Destination NAI field 204 identifies the destination of the message as the AAA Entity 1 of Domain A, since the AAA Entity 1 of Domain A sent the Registration Request message 200. The User NAI field 206 identifies the user that originated the request, which in this example is user1, who has a home domain of the Domain B. The Command Code field 208 identifies the type of message as a message 200 responding to a request for registration.

Referring again to FIGURE 3, routing of a message 200 responding to a request for registration is illustrated. In step 302, the AAA Server of Domain B receives the Registration message 200 requesting registration from the AAA Entity 1 of Domain B. Execution then proceeds to step 304, wherein a determination is made whether a Destination NAI is present in the field 204. If it is determined that a Destination NAI (*e.g.*, aaaentity1@DomainA) is present in the

field 204, then execution proceeds to step 306; otherwise, execution proceeds to step 308, discussed above with respect to transmission of a message requesting registration. In step 306, a determination is made whether the Destination NAI field 204 identifies a local domain. If it is determined that the Destination NAI field 204 does not identify a local domain, execution proceeds to step 314; otherwise, execution proceeds to step 310, discussed below. In step 314, the IP address of the Destination NAI field 204 is determined using the well-known DNS. Execution then proceeds to step 316, wherein the AAA Server of Domain B dispatches the message 200 responding to a request for registration to the proper AAA domain, which, in the present example, is the AAA Server of Domain A because the domain portion of the Destination NAI field 204 identifies the Domain A. Execution then returns to step 302.

In step 302, the AAA Server of Domain A receives the Registration Response message 200 that was dispatched in step 316 from the AAA Server of Domain B. Execution then proceeds to step 304, wherein a determination is made whether a Destination NAI (*e.g.*, aaaentity1@DomainA) is present in the field 204. If it is determined that a Destination NAI is present in the field 204, then execution proceeds to step 306; otherwise, execution proceeds to step 308, discussed above with respect to transmission of a message requesting registration. In step 306, the AAA Server of Domain A determines whether the Destination NAI field 204 identifies a local domain. If it is determined that the Destination NAI field 204 identifies a local domain (*e.g.*, DomainA), then execution proceeds to step 310; otherwise, execution proceeds to step 314, discussed above. In step 310, a determination is made to which AAA entity (*e.g.*, AAA Entity 1 of Domain A) the Registration Response message 200 should be dispatched. It will be apparent to

those skilled in the art that, unlike prior art approaches, even if the AAA entity to which the Registration message 200 response is directed has only a private IP address, the message 200 can be routed to the proper entity, so long as the AAA Server serving the entity has a publicly routable address.

From step 310, execution proceeds to step 312. In step 312, the AAA Server of the Domain A dispatches the message 200 to the proper AAA entity of the local domain (*e.g.*, AAA Entity 1 of Domain A). Execution then terminates at step 328.

By use of the present invention, routing of AAA messages of roaming users is achievable, messaging between a AAA entity to another AAA entity in any domain can be performed, and communication between two or more non-home serving domains can be accomplished in a system using any AAA protocol. In addition, the present invention provides an apparatus and method that permits communications between two specific entities in different domains as well as communications between entities in which one or more of the entities is behind a firewall or a proxy server and thus does not have a publicly-routable IP address. The present invention also allows servers to be stateless and lightweight (since message routing state information need not be stored in the servers).

It is understood that the present invention can take many forms and embodiments. Accordingly, several variations may be made in the foregoing without departing from the spirit or the scope of the invention. For example, various algorithms in addition to the that disclosed herein could be devised using the destination NAI to route AAA messages among different domains of a network.

Although the invention has been described with specific AAA protocol embodiments, these descriptions are not meant

to be construed in a limiting sense. Various modifications of the disclosed embodiments, as well as alternative embodiments of the invention, will become apparent to persons skilled in the art upon reference to the description of the invention. It is, therefore, contemplated that the claims will cover any such modifications or embodiments that fall within the true scope and spirit of the invention.

WHAT IS CLAIMED IS:

1. A method for facilitating authentication, authorization, and accounting (AAA) message routing by an AAA server comprising the steps of:

receiving an AAA message having at least a user network address identifier (NAI);

determining whether the AAA message includes a destination NAI;

in response to a determination that the AAA message includes a destination NAI, determining whether an NAI domain of the destination NAI is local;

in response to a determination that the destination NAI is local, determining from the destination NAI a local AAA entity to which the AAA message should be dispatched and dispatching the AAA message to the determined local AAA entity; and

in response to a determination that the destination NAI is not local, resolving an internet protocol (IP) address of the destination NAI and dispatching the AAA message to an AAA server in a non-local domain identified by the destination NAI.

2. The method of claim 1 wherein the AAA server is stateless.

3. The method of claim 1 further comprising the step of retrieving the user NAI in response to a determination that the AAA message does not include a destination NAI.

4. The method of claim 3 further comprising the step of determining whether a NAI domain of the user NAI of the AAA message is local.

5. The method of claim 4 further comprising the step of determining a local AAA entity to which the AAA message should be dispatched from a message type of the AAA message in response to a determination that the NAI domain of the user NAI of the AAA message is local.

6. The method of claim 4 further comprising the step of resolving an IP address of the user NAI in response to a determination that the NAI domain of the user NAI of the AAA message is not local.

7. The method of claim 5 further comprising the step of dispatching the AAA message to a proper local AAA entity.

8. The method of claim 6 further comprising the step of dispatching the AAA message to a proper non-local domain.

9. The method of claim 8 wherein at least one of the AAA entities does not have a publicly routable IP address.

10. A method of facilitating routing of an AAA registration request message comprising the steps of:

receiving an AAA registration request message having at least a user NAI;

determining whether a NAI domain of the user NAI is local;

in response to a determination that the NAI domain is

local, dispatching the message to a local entity identified by the user NAI; and

in response to a determination that the NAI domain is non-local, dispatching the message to a non-local domain identified by the user NAI.

11. A method of facilitating routing of an AAA registration response message comprising the steps of:

receiving an AAA registration response message having at least a destination NAI;

determining whether the NAI domain of the destination NAI is local;

in response to a determination that the NAI domain of the destination NAI is local, dispatching the message to a local AAA entity identified by the destination NAI; and

in response to a determination that the NAI domain of the destination NAI is not local, dispatching the message to an AAA domain identified by the destination NAI.

12. The method of claim 10 wherein the local AAA entity has a private IP address.

13. The method of claim 11 wherein the local AAA entity has a private IP address.

14. An apparatus for routing of Authentication, Authorization, and Accounting (AAA) messages between AAA entities comprising:

a first domain operably connected to a data network, the first domain having at least one first AAA server, the first AAA server being adapted to route a plurality of AAA messages having a source NAI and a user NAI; and

a first AAA entity operably connected to the first domain, the first AAA entity being adapted to send and receive a plurality of AAA messages, each message having at least a source NAI and a user NAI.

15. The apparatus of claim 14 further comprising:

a second domain operably connected to a data network, the second domain having at least one second AAA server, the second AAA server being adapted to route a plurality of AAA messages having a source NAI and a user NAI;

a second AAA entity operably connected to the second domain, the second AAA entity being adapted to send and receive a plurality of AAA messages, each message having at least a source NAI and a user NAI.

16. The apparatus of claim 14 further comprising a computer program product having a medium with a computer program embodied thereon, the computer program comprising computer program code executable, in response to receipt of an AAA message, for routing the AAA message, the computer program further comprising:

computer program code for determining whether a destination network access identifier (NAI) is present in the AAA message;

computer code for determining, in response to a determination that a destination NAI is present in the AAA message, whether an NAI domain of the destination NAI is local;

computer code for determining, in response to a determination that the NAI domain of the destination NAI is local, a local AAA entity to which the message should be

dispatched; and

computer code for dispatching the AAA message to the local AAA entity in response to the determination of the local AAA entity to which the message should be dispatched.

17. The apparatus of claim 14 further comprising a computer program product having a medium with a computer program embodied thereon, the computer program comprising computer program code executable, in response to receipt of an AAA message, for routing the AAA message, the computer program further comprising:

computer program code for determining whether a destination network access identifier (NAI) is present in the AAA message;

computer code for determining, in response to a determination that a destination NAI is present in the AAA message, whether an NAI domain of the destination NAI is local;

computer code for determining, in response to a determination that the NAI domain of the destination NAI is local, a local AAA entity to which the message should be dispatched;

computer code for dispatching the AAA message to the local AAA entity in response to determination of the local AAA entity to which the message should be dispatched;

computer code for resolving an internet protocol (IP) address of the NAI domain of the destination NAI in response to a determination that the destination NAI is not local; and

computer code for dispatching the AAA message to the NAI domain of the destination NAI in response to resolution of the IP address of the NAI domain.

18. The apparatus of claim 14 further comprising a computer program product having a medium with a computer program embodied thereon, the computer program comprising computer program code executable, in response to receipt of an AAA message, for routing the AAA message, the computer program further comprising:

computer program code for determining whether a destination network access identifier (NAI) is present in the AAA message;

computer code for determining, in response to a determination that a destination NAI is present in the AAA message, whether an NAI domain of the destination NAI is local;

computer code for determining, in response to a determination that the NAI domain of the destination NAI is local, a local AAA entity to which the message should be dispatched;

computer code for dispatching the AAA message to the local AAA entity in response to identification of the local AAA entity to which the message should be dispatched;

computer code for resolving an internet protocol (IP) address of the NAI domain of the destination NAI in response to a determination that the destination NAI is not local;

computer code for dispatching the AAA message to the NAI domain of the destination NAI in response to resolution of the IP address of the NAI domain of the destination NAI;

computer code for retrieving a user NAI from the AAA message in response to a determination that a destination NAI is not present in the AAA message;

computer code for determining, in response to retrieval of the user NAI from the AAA message, whether the NAI domain

of the user NAI is local;

computer code for determining, in response to a determination that the NAI domain of the user NAI of the AAA message is local, a local AAA entity to which the AAA message should be dispatched; and

computer code for dispatching the AAA message to the local AAA entity in response to the determination of the local AAA entity to which the AAA message should be dispatched. The apparatus of claim 14 further comprising a computer program product having a medium with a computer program embodied thereon, the computer program comprising computer program code executable, in response to receipt of an AAA message, for routing the AAA message, the computer program further comprising:

computer program code for determining whether a destination network access identifier (NAI) is present in the AAA message;

computer code for determining, in response to a determination that a destination NAI is present in the AAA message, whether an NAI domain of the destination NAI is local;

computer code for determining, in response to a determination that the NAI domain of the destination NAI is local, a local AAA entity to which the message should be dispatched;

computer code for dispatching the AAA message to the local AAA entity in response to identification of the local AAA entity to which the message should be dispatched;

computer code for resolving an internet protocol (IP) address of the NAI domain of the destination NAI in response to a determination that the destination NAI is not local;

computer code for dispatching the AAA message to the NAI domain of the destination NAI in response to resolution of the IP address of the NAI domain of the destination NAI;

computer code for retrieving a user NAI from the AAA message in response to a determination that a destination NAI is not present in the AAA message;

computer code for determining, in response to retrieval of the user NAI from the AAA message, whether the NAI domain of the user NAI is local;

computer code for determining, in response to a determination that the NAI domain of the user NAI of the AAA message is local, a local AAA entity to which the AAA message should be dispatched;

computer code for dispatching the AAA message to the local AAA entity in response to the determination of the local AAA entity to which the AAA message should be dispatched;

computer code for resolving an IP address of the NAI domain of the user NAI in response to a determination that the NAI domain of the user NAI is not local; and

computer code for dispatching the AAA message to the NAI domain of the user NAI in response to resolution of the IP address of the NAI domain of the user NAI.

19. The apparatus of claim 14 wherein the first domain is a non-home serving domain.

20. The apparatus of claim 14 wherein a portion of the AAA messages are registration request messages. The apparatus of claim 14 wherein a portion of the AAA messages are registration response messages that include a destination NAI. The apparatus of claim 14 wherein at least one of the AAA

entities has a private IP address. The apparatus of claim 15 wherein at least one of the AAA servers is stateless. The apparatus of claim 15 wherein the second domain is a non-home serving domain.

21. The apparatus of claim 15 wherein a portion of the AAA messages are registration request messages.

22. The apparatus of claim 15 wherein a portion of the AAA messages are response messages that include a destination NAI. The apparatus of claim 15 wherein at least one of the AAA entities has a private IP address.

23. The apparatus of claim 15 further comprising a computer program product having a medium with a computer program embodied thereon, the computer program comprising computer program code executable, in response to receipt of an AAA message, for routing the AAA message, the computer program further comprising:

computer program code for determining whether a destination network access identifier (NAI) is present in the AAA message;

computer code for determining, in response to a determination that a destination NAI is present in the AAA message, whether an NAI domain of the destination NAI is local;

computer code for determining, in response to a determination that the NAI domain of the destination NAI is local, a local AAA entity to which the message should be dispatched; and

computer code for dispatching the AAA message to the local AAA entity in response to the determination of the local

AAA entity to which the message should be dispatched.

24. The apparatus of claim 15 further comprising a computer program product having a medium with a computer program embodied thereon, the computer program comprising computer program code executable, in response to receipt of an AAA message, for routing the AAA message, the computer program further comprising:

computer program code for determining whether a destination network access identifier (NAI) is present in the AAA message;

computer code for determining, in response to a determination that a destination NAI is present in the AAA message, whether an NAI domain of the destination NAI is local;

computer code for determining, in response to a determination that the NAI domain of the destination NAI is local, a local AAA entity to which the message should be dispatched;

computer code for dispatching the AAA message to the local AAA entity in response to determination of the local AAA entity to which the message should be dispatched;

computer code for resolving an internet protocol (IP) address of the NAI domain of the destination NAI in response to a determination that the destination NAI is not local; and

computer code for dispatching the AAA message to the NAI domain of the destination NAI in response to resolution of the IP address of the NAI domain.

25. The apparatus of claim 15 further comprising a computer program product having a medium with a computer

program embodied thereon, the computer program comprising computer program code executable, in response to receipt of an AAA message, for routing the AAA message, the computer program further comprising:

computer program code for determining whether a destination network access identifier (NAI) is present in the AAA message;

computer code for determining, in response to a determination that a destination NAI is present in the AAA message, whether an NAI domain of the destination NAI is local;

computer code for determining, in response to a determination that the NAI domain of the destination NAI is local, a local AAA entity to which the message should be dispatched;

computer code for dispatching the AAA message to the local AAA entity in response to identification of the local AAA entity to which the message should be dispatched;

computer code for resolving an internet protocol (IP) address of the NAI domain of the destination NAI in response to a determination that the destination NAI is not local;

computer code for dispatching the AAA message to the NAI domain of the destination NAI in response to resolution of the IP address of the NAI domain of the destination NAI;

computer code for retrieving a user NAI from the AAA message in response to a determination that a destination NAI is not present in the AAA message;

computer code for determining, in response to retrieval of the user NAI from the AAA message, whether the NAI domain of the user NAI is local;

computer code for determining, in response to a

determination that the NAI domain of the user NAI of the AAA message is local, a local AAA entity to which the AAA message should be dispatched; and

computer code for dispatching the AAA message to the local AAA entity in response to the determination of the local AAA entity to which the AAA message should be dispatched. The apparatus of claim 15 further comprising a computer program product having a medium with a computer program embodied thereon, the computer program comprising computer program code executable, in response to receipt of an AAA message, for routing the AAA message, the computer program further comprising:

computer program code for determining whether a destination network access identifier (NAI) is present in the AAA message;

computer code for determining, in response to a determination that a destination NAI is present in the AAA message, whether an NAI domain of the destination NAI is local;

computer code for determining, in response to a determination that the NAI domain of the destination NAI is local, a local AAA entity to which the message should be dispatched;

computer code for dispatching the AAA message to the local AAA entity in response to identification of the local AAA entity to which the message should be dispatched;

computer code for resolving an internet protocol (IP) address of the NAI domain of the destination NAI in response to a determination that the destination NAI is not local;

computer code for dispatching the AAA message to the NAI domain of the destination NAI in response to resolution of the

IP address of the NAI domain of the destination NAI;

computer code for retrieving a user NAI from the AAA message in response to a determination that a destination NAI is not present in the AAA message;

computer code for determining, in response to retrieval of the user NAI from the AAA message, whether the NAI domain of the user NAI is local;

computer code for determining, in response to a determination that the NAI domain of the user NAI of the AAA message is local, a local AAA entity to which the AAA message should be dispatched;

computer code for dispatching the AAA message to the local AAA entity in response to the determination of the local AAA entity to which the AAA message should be dispatched;

computer code for resolving an IP address of the NAI domain of the user NAI in response to a determination that the NAI domain of the user NAI is not local; and

computer code for dispatching the AAA message to the NAI domain of the user NAI in response to resolution of the IP address of the NAI domain of the user NAI. An AAA message comprising a source network access identifier that indicates a source AAA entity from which the AAA message has been sent. The AAA message of claim 33 further comprising a destination network access identifier that indicates a destination to which the message is to be sent.

26. The AAA message of claim 34 further comprising a user network access identifier that indicates a user's name and the user's home domain.

27. The AAA message of claim 35 further comprising a

command code that indicates what type of action should be taken in response to the message.

FIG. 1
PRIOR ART

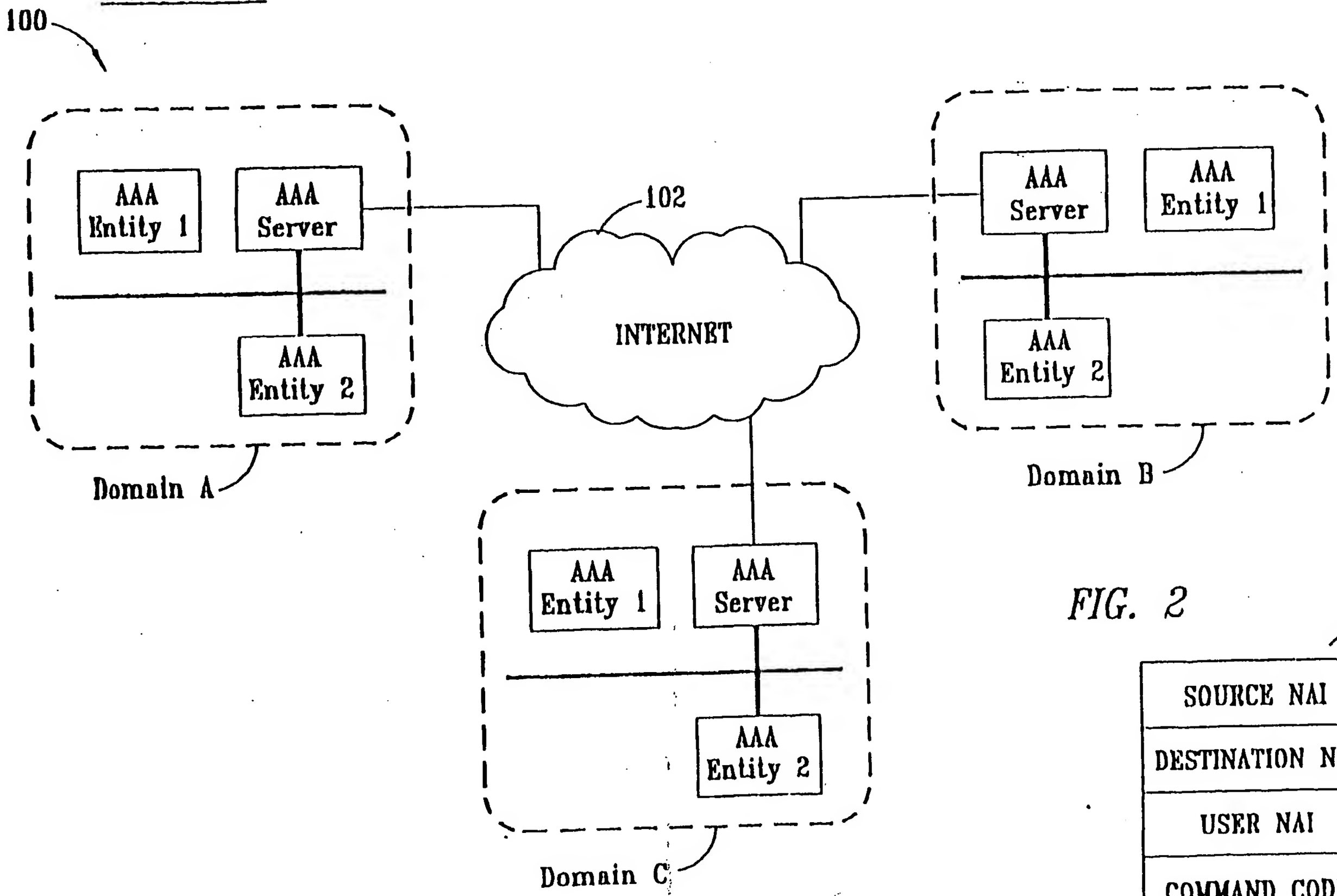
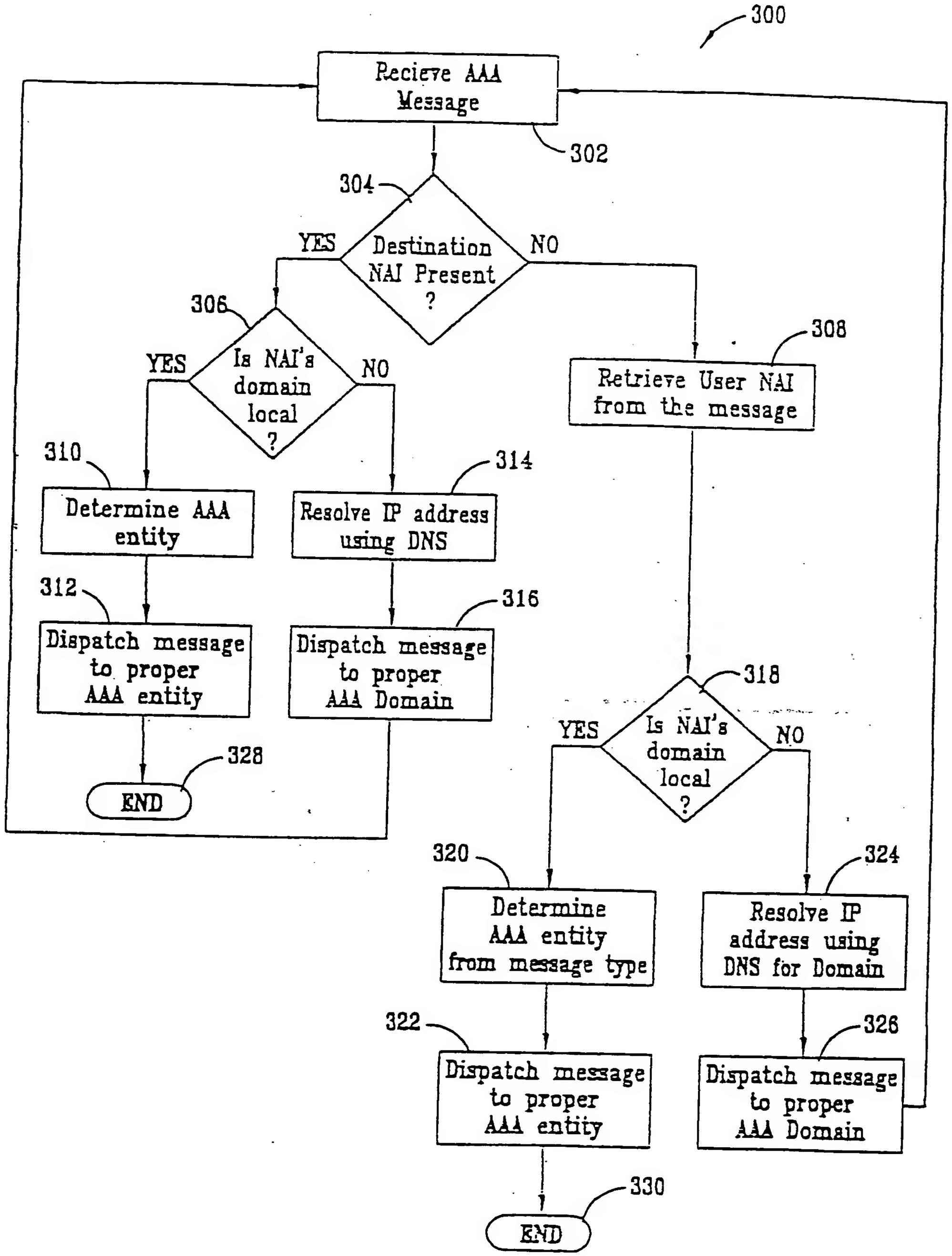


FIG. 2


300
Recieve AAA Message
302
304
Destination NAI Present ?
YES
NO
306
Is NAI's domain local ?
YES
NO
308
Retrieve User NAI from the message
310
Determine AAA entity
314
Resolve IP address using DNS
312
Dispatch message to proper AAA entity
316
Dispatch message to proper AAA Domain
328
END
318
Is NAI's domain local ?
YES
NO
320
Determine AAA entity from message type
324
Resolve IP address using DNS for Domain
322
Dispatch message to proper AAA entity
326
Dispatch message to proper AAA Domain
330
END

INTERNATIONAL SEARCH REPORT

Interr nal Application No
PCT/IB 00/01304

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	"Multimedia Conference Manager" RELEASE 11.3 NA, 4 March 1999 (1999-03-04), XP002152853 page 1, line 1 -page 2, line 5	1,2
Y	page 13, paragraph 4	3,4,6,8
A		14-27

X	EP 0 912 026 A (LUCENT TECHNOLOGIES INC) 28 April 1999 (1999-04-28) abstract	10,11
Y	page 11, paragraph 73	3,4,6,8
A	page 16, paragraph 104 - paragraph 107 page 22, paragraph 155 - paragraph 156 page 27, paragraph 178	14-27

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance.

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 January 2001	22/01/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Blanco Cardona, P

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inten nal Application No
PCT/IB 00/01304

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	WO 99 39481 A (IP DYNAMICS INC) 5 August 1999 (1999-08-05) abstract page 4, paragraph 4 -page 5, paragraph 1 page 17, line 15 - line 23	9,12-14, 22
A	JOHNSON ET AL: "A Global Alphanumeric Naming Scheme for H.323" REQUEST FOR COMMENT, 12 July 1999 (1999-07-12), XP002152855 the whole document	1-8,10, 11

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter nal Application No
PCT/IB 00/01304

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0912026 A	28-04-1999	CA 2249817 A	14-04-1999
		CA 2249830 A	14-04-1999
		CA 2249831 A	14-04-1999
		CA 2249836 A	14-04-1999
		CA 2249837 A	14-04-1999
		CA 2249838 A	14-04-1999
		CA 2249839 A	14-04-1999
		CA 2249862 A	14-04-1999
		CA 2249863 A	14-04-1999
		EP 0910198 A	21-04-1999
		EP 0917320 A	19-05-1999
		EP 0917318 A	19-05-1999
		EP 0912027 A	28-04-1999
		EP 0912012 A	28-04-1999
		EP 0917328 A	19-05-1999
		EP 0918417 A	26-05-1999
		EP 0912017 A	28-04-1999
		JP 11289353 A	19-10-1999
		JP 11252183 A	17-09-1999
		JP 11275154 A	08-10-1999
		JP 11275155 A	08-10-1999
		JP 2000022758 A	21-01-2000
		JP 11275156 A	08-10-1999
		JP 11275157 A	08-10-1999
		JP 11284666 A	15-10-1999
		JP 11331276 A	30-11-1999
WO 9939481 A	05-08-1999	US 6119171 A	12-09-2000
		AU 2347099 A	16-08-1999
		EP 1057309 A	06-12-2000